DIGITAL DEFENCE

Incident Response and Management:

1st Responder's Workshop

Respond
Service

DigitalDefence's 2-day workshop for First Responders to is a hands-on look at how data security incidents are caused, how to recognize them, and how to resolve them with minimum financial and reputational loss

The First Responder in a data security incident plays a pivotal role – they will be the one who first recognizes that an attack is taking place, and will put into place the steps that will stop the attacking, minimizing your financial loss and damage to your data.

DigitalDefence's workshop for 1st Responders is a hands-on look at how incidents are caused, how to recognize them, and how to resolve them.

A core component of the program is unique scenario-based training based on real Canadian security incidents.

We attend security conferences around the world, and work with the open source community to develop and refine security tools. Because of this, you can be certain that you will receive the latest cutting edge material during the workshop.

WHAT YOU WILL LEARN

- How to effectively plan in advance for a security incident, ensuring organizational readiness
- How to effectively respond to an incident, and avoid common –and costly—mistakes
- How to gather the information needed for root-cause analysis and support legal action
- How to manage the response process
- How to satisfy regulatory requirements under HIPAA / HITECH ISO 27001, PCI DSS, Sarbanes-Oxley, and other frameworks

Reduce corporate risks with focused incident response training.

Is the 1st Responder's Workshop right for your company?

- Do you need to reduce financial losses due to business downtime?
- Do you need to manage your liability and insurance costs?
- Are you prepared to recognize and respond to a data security breach?
- Should a breach occur, do you know who you have to notify, and when?
- Will your business survive and recover from a network attack?
- Are you meeting your regulatory requirements for incident response?

COURSE OVERVIEW

- Introduction to attackers (external, external), the threat environment
- Review of attacker methodologies, with hands-on demonstrations and practice in implementing the most common attacks
- Recognizing a data security incident (internal and external origins)
- Planning including resource management, responsibility and authority delegation
- The incident response process, covering development of internal standard operating procedures, the computer security incident response team (CSIRT), notification and escalation processes, internal communications and public relations, reporting, lessons learned
- Reporting a security breach internally, and to clients, regulators, and government
- Responding to common attacks (scenario-based training)
- Collecting data from a live system
- Supporting the collection of forensic evidence and litigation preparation
- Relevant laws and regulations

We believe that theoretical instruction must be accompanied with practical drills based on real-world examples of security incidents; this is the only way to instill the confidence needed by response staff.

Therefore, we use realistic training scenarios that include: non-compliance with the corporate information security policy; recon activity against the network (e.g.: vulnerability scanning); website defacement; denial of service, DoS, attacks; attack by a hacker; attack by malicious software; theft or loss of a mobile device; and, data ransom and extortion.

Our scenarios also deal with recognizing and responding to internal HR issues such as false employee claims, harassment, inappropriate online activity, electronic sabotage, and employee fraud.

The workshop can be delivered at your site, reducing travel costs, minimizing work disruptions, and creating a private atmosphere to discuss the security of your specific business.

Who Should Attend

This workshops intended for those who need to be proficient at recognizing and responding to data security incidents, and preserving and analyzing evidence (system and network administrators, database administrators, security and privacy specialists).

This course is also pertinent for HR managers and others who conduct internal investigations.

About DigitalDefence

DigitalDefence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

Disclaimer

This document is for informational purposes only. DigitalDefence makes no warranties, express or implied, in this document.